

EXHIBIT 1

SUPERIOR COURT
BARNSTABLE, SS 1

DEC 08 2022

FILED

Scott W. Nickerson, Clerk

COMMONWEALTH OF MASSACHUSETTS

BARNSTABLE, S.S.

SUPERIOR COURT

JANE DOE,
INDIVIDUALLY AND ON
BEHALF OF ALL OTHERS SIMILARLY
SITUATED,

Plaintiff

v.

CAPE COD HEALTHCARE, INC.,

Defendant.

C.A. No.

~~22CV493~~

23-1236-BLS1

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Jane Doe ("Plaintiff"), individually and on behalf of all other persons similarly situated, brings suit against Defendant Cape Cod Healthcare, Inc. d/b/a Cape Cod Hospital, Falmouth Hospital, and JML Care Center ("Defendant"), and upon personal knowledge as to Plaintiff's own conduct and on information and belief as to all other matters based upon investigation by counsel, alleges as follows:

NATURE OF ACTION AND ALLEGATIONS

1. This case arises from Defendant's systematic violation of the medical privacy rights of its patients, exposing highly sensitive personal information to third parties without those patients' knowledge or consent.

2. Defendant's "Privacy Policy" tells patients that "[a]t Cape Code Healthcare, we are committed to protecting the privacy and security of the users of our internet site."¹ Indeed, Defendant assures patients that it is "committed to protecting the identities of visitors to our site"

¹ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

and that, other than disclosing personal information to process credit card information, it ‘has no other current plans to make other disclosures of such information.’”² Contrary to these assurances, however, Defendant does not follow these policies, nor the law prohibiting such disclosures.

3. At all relevant times, Defendant disclosed information about its patients—including their status as patients, their physicians, their medical treatments, the hospitals they visited, and their personal identities—to Facebook and other third parties without their patients’ knowledge, authorization, or consent.

4. Defendant discloses this protected health information through the deployment of various digital marketing and automatic rerouting tools embedded on its websites that purposefully and intentionally redirect patients’ personal health information to third parties who exploit that information for advertising purposes. Defendant’s use of these rerouting tools causes its patients’ personally identifiable information and the contents of its patients’ communications exchanged with Defendant to be automatically redirected to third parties in violation of those patients’ reasonable expectations of privacy, their rights as patients, their rights as citizens of Massachusetts, and both the express and implied promises of Defendant.

5. Defendant’s conduct in disclosing such protected health information about its patients to Facebook and other third parties violates Massachusetts law, including G.L. c. 272, § 99 (Interception of Wire and Oral Communications), G.L. c.214, § 1B (Right to Privacy), and G.L. c. 111, § 70E (Patients’ and Residents’ Rights).

6. On behalf of herself and all similarly situated persons, Plaintiff seeks an order enjoining Defendant from further unauthorized disclosures of her personal information; awarding

² <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

liquidated damages in the amount of \$1,000 per violation, attorney's fees and costs; and granting any other preliminary or equitable relief the Court deems appropriate.

PARTIES TO THE ACTION

7. Defendant Cape Cod Healthcare, Inc. is a Massachusetts corporation with its principal office at 27 Park Street, Hyannis, MA 02601. Defendant is a private health system providing healthcare services for residents and visitors of Cape Cod.³ Defendant owns and manages numerous healthcare facilities in Massachusetts, including Cape Cod Hospital, Falmouth Hospital, JML Health Care Center, Cape Cod Surgery Center, Davenport-Mugar Cancer Center, Falmouth Hospital Rehabilitation Center, Cape Cod Healthcare Urgent Care-Falmouth, Cape Cod Healthcare Urgent Care-Harwich, and Cape Cod Healthcare Pharmacy.⁴

8. Plaintiff, Jane Doe, has a residence in Barnstable County, Massachusetts, has been treated by Defendant's physicians, and has been a patient Cape Cod Hospital,⁵ and thus also a patient of Defendant.

JURISDICTION AND VENUE

9. This Court has personal jurisdiction over Defendant because it regularly conducts business throughout Massachusetts and has its principal place of business at 27 Park Street, Hyannis, Massachusetts, 02601. G.L. c. 223A, § 2; G.L. c. 223A, § 3.

10. Venue is appropriate in this Court because Defendant resides in Barnstable County and the acts or conduct giving rise to the cause of action took place in Barnstable County. G.L. c. 223, § 1.

³ <https://www.capecodhealth.org/about/>

⁴ <https://www.capecodhealth.org/locations/>

⁵ <https://www.capecodhealth.org/locations/profile/cape-cod-hospital/?searchId=db38b971-ab75-ed11-a85a-000d3a611c21&sort=11&page=1&pageSize=10>

FACTUAL BACKGROUND

A. Defendant routinely discloses the protected health information of its patients to third parties including Facebook.

11. Plaintiff Jane Doe is a patient of Defendant who has received treatment from Defendant at Cape Cod Hospital.⁶

12. Under G.L. c. 214, § 1B, all persons “have a right against unreasonable, substantial, or serious interference” with their privacy.

13. Medical patients in Massachusetts such as Jane Doe have a legal interest in preserving the confidentiality of their communications with healthcare providers and have reasonable expectations of privacy that their personally identifiable information and communications will not be disclosed to third parties by Defendant without their express written consent and authorization.

14. As a health care provider, Defendant has fiduciary, common law, and statutory duties to protect the confidentiality of patient information and communications.

15. Defendant expressly and impliedly promises patients that it will maintain and protect the confidentiality of personally identifiable patient information and communications.

16. Defendant operates websites for patients, including www.capecodhealth.org.

17. Defendant’s websites are designed for interactive communication with patients, including scheduling appointments, searching for physicians, paying bills, requesting medical records, learning about medical issues treatment options, and joining support groups.

18. Notwithstanding patients’ reasonable expectations of privacy, Defendant’s legal duties of confidentiality, and Defendant’s express promises to the contrary, Defendant discloses the contents of patients’ communications and protected healthcare information via automatic re-

⁶ <https://www.capecodhealth.org/locations/profile/cape-cod-hospital/?searchId=db38b971-ab75-ed11-a85a-000d3a611c21&sort=11&page=1&pageSize=10>

routing mechanisms embedded in the website operated by Defendant without patients' knowledge, authorization, or consent.

B. The nature of Defendant's unauthorized disclosure of patients' health care information.

19. Defendant's disclosures of patients' personal healthcare information occur because Defendant intentionally deploys source code on the websites it operates, including www.capecodhealth.org, that causes patients' personally identifiable information (as well as the exact contents of their communications) to be transmitted to third parties.

20. By design, third parties receive and record the exact contents of patient communications before the full response from Defendant to patients has been rendered on the screen of the patient's computer device and while the communication between Defendant and the patient remains ongoing.

21. Websites like those maintained by Defendant are hosted by a computer server through which the business in charge of the website exchanges and communicates with internet users via their web browsers.

22. The basic command that web browsers use to exchange data and user communications is called a GET request.⁷ For example, when a patient types "heart failure treatment" into the search box on Defendant's website and hits 'Enter,' the patient's web browser makes a connection with the server for Defendant's website and sends the following request: "GET search/q=heart+failure+treatment."

23. The other basic transmission command utilized by web browsers is POST, which is typically employed when a user enters data into a form on a website and clicks 'Enter' or some

⁷ https://www.w3schools.com/tags/ref_httpmethods.asp

other form of submission button. POST sends the data entered in the form to the server hosting the website that the user is visiting.

24. In response to receiving a GET or POST command, the server for the website with which the user is exchanging information will send a set of instructions to the web browser and command the browser with source code that directs the browser to render the website's responsive communication.

25. Unbeknownst to most users, however, the website's server may also redirect the user's communications to third parties. Typically, users are given no notice that these disclosures are being made. Third parties (such as Facebook and Google) use the information they receive to track user data and communications for marketing purposes.

26. In many cases, third-party marketing companies acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screen) called a tracking pixel, a web-bug, or a web beacon. These tracking pixels are tiny and are purposefully camouflaged to remain invisible to users.

27. Tracking pixels can be placed directly on a web page by a developer, or they can be funneled through a "tag manager" service to make the invisible tracking run more smoothly. A tag manager further obscures the third parties to whom user data is transmitted.

28. These tracking pixels can collect dozens of data points about individual website users who interact with a website. One of the world's most prevalent tracking pixels, called the Meta Pixel, is provided by Facebook.

29. A web site developer who chooses to deploy third-party source code, like a tracking pixel, on their website must enter the third-party source code directly onto their website

for every third party they wish to send user data and communications. This source code operates invisibly in the background when users visit a site employing such code.

C. Tracking pixels provide third parties with a trove of personally identifying data permitting them to uniquely identify the individuals browsing a website.

30. Tracking pixels are lines of source code embedded in websites such as Defendant's. Tracking pixels are particularly pernicious because they result in the disclosure of a variety of data that permits third parties to determine the unique personal identities of website visitors. While most users believe that the internet provides them with anonymity when, for example, they browse a hospital website for treatment information about a medical condition, that is not the case when the hospital website has embedded third party tracking devices, as Defendant has.

31. For example, an IP address is a number that identifies a computer connected to the internet. IP addresses are used to identify and route communications on the internet. IP addresses of individual users are used by internet service providers, websites, and tracking companies to facilitate and track internet communications and content. IP addresses also offer advertising companies like Facebook a unique and semi-persistent identifier across devices—one that has limited privacy controls.⁸

32. Because of their uniquely identifying character, IP address are considered protected personally identifiable information. Tracking pixels can (and typically do) collect website visitors' IP addresses.

33. Likewise, internet cookies also provide personally identifiable information. Cookies are small text files that web servers can place on a user's browser and computer when a user's browser interacts with a website server. Cookies are typically designed to acquire and

⁸ <https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/>

record an individual internet user's communications and activities on websites and were developed by programmers to aid with online advertising.

34. Cookies are designed to operate as a means of identification for internet users. Advertising companies like Facebook and Google have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell targeted advertising that is customized to a user's personal communications and browsing history. To build individual profiles of internet users, third party advertising companies assign each user a unique (or a set of unique) identifiers to each user.

35. Cookies are considered personal identifiers protected, and tracking pixels can collect cookies from website visitors.

36. A third type of personally identifying information is what data companies refer to as a "browser-fingerprint." A browser-fingerprint is information collected about a computing device that can be used to identify the specific device.

37. These browser-fingerprints can be used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data. As Google explained, "With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."⁹ The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it

⁹ <https://www.blog.google/products/chrome/building-a-more-private-web/>

employs much more subtle techniques.¹⁰ Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.¹¹

38. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.¹²

39. Browser-fingerprints are considered personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors.

40. A fourth kind of personally identifying information is the unique user identifier (such as Facebook's "Facebook ID") that permits companies like Facebook to quickly and automatically identify the personal identity of its user across the internet whenever the identifier is encountered. A Facebook ID is a number string that is connected to a user's Facebook profile.¹³ Anyone with access to a user's Facebook ID can locate a user's Facebook profile.¹⁴

41. Unique personal identifiers such as a person's Facebook are likewise capable of collection through pixel trackers.

D. Facebook

42. Facebook, a social media platform founded in 2004 and today operated by Meta Platforms, Inc., was originally designed as a social networking website for college students.

43. Facebook describes itself as a "real identity" platform.¹⁵ This means that users are permitted only one account and must share "the name they go by in everyday life."¹⁶ To that end, Facebook requires users to provide their first and last name, along with their birthday,

¹⁰ <https://pixelprivacy.com/resources/browser-fingerprinting/>

¹¹ <https://www.blog.google/products/chrome/building-a-more-private-web/>

¹² <https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/>

¹³ <https://www.facebook.com/help/211813265517027>

¹⁴ <https://smallseotools.com/find-facebook-id/>

¹⁵ <https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701#:~:text=Facebook%20said%20in%20its%20most,of%20them%20than%20developed%20ones.>

¹⁶ <https://transparency.fb.com/policies/community-standards/account-integrity-and-authentic-identity/>

telephone number and/or email address, and gender, when creating an account.¹⁷

44. In 2007, realizing the value of having direct access to millions of consumers, Facebook began monetizing its platform by launching “Facebook Ads,” proclaiming this service to be a “completely new way of advertising online,” that would allow “advertisers to deliver more tailored and relevant ads.”¹⁸ Facebook has since evolved into one of the largest advertising companies in the world.¹⁹ Facebook can target users so effectively because it surveils user activity both on and off its website through the use of tracking pixels.²⁰ This allows Facebook to make inferences about users based on their interests, behavior, and connections.²¹

45. Today, Facebook provides advertising on its own social media platforms, as well as other websites through its Facebook Audience Network. Facebook has more than 2.9 billion users.²²

46. Facebook maintains profiles on users that include users’ real names, locations, email addresses, friends, likes, and communications. These profiles are associated with personal identifiers, including IP addresses, cookies, and other device identifiers. Facebook also tracks non-users across the web through its internet marketing products and source code.

47. Facebook offers several advertising options based on the type of audience that an advertiser wants to target. Those options include targeting “Core Audiences,” “Custom Audiences,” “Look Alike Audiences,” and even more granulated approaches within audiences called “Detailed Targeting.” Each of Facebook’s advertising tools allow an advertiser to target users based, among other things, on their personal data, including geographic location,

¹⁷ <https://www.facebook.com/help/406644739431633>

¹⁸ <https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/>

¹⁹ <https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/>

²⁰ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

²¹ <https://www.facebook.com/business/ads/ad-targeting>

²² <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>

demographics (e.g., age, gender, education, job title, etc.), interests, (e.g., preferred food, movies), connections (e.g., particular events or Facebook pages), and behaviors (e.g., purchases, device usage, and pages visited). This audience can be created by Facebook, the advertiser, or both working in conjunction.

48. Ad Targeting has been extremely successful due to Facebook's ability to target individuals at a granular level. For example, among many possible target audiences, "Facebook offers advertisers 1.5 million people 'whose activity on Facebook suggests that they're more likely engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"²³ Aided by highly granular data used to target specific users, Facebook's advertising segment quickly became Facebook's most successful business unit, with millions of companies and individuals utilizing Facebook's advertising services.

E. Facebook's Meta Pixel tool allows Facebook to track the personal data of individuals across a broad range of third-party websites.

49. To power its advertising business, Facebook uses a variety of tracking tools to collect data about individuals, which it can then share with advertisers. These tools include software development kits incorporated into third-party applications, its "Like" and "Share" buttons (known as "social plug-ins"), and other methodologies, which it then uses to power its advertising business.

50. One of Facebook's most powerful tools is called the "Meta Pixel."

51. The Meta Pixel is a snippet of code embedded on a third-party website that tracks users' activities as users navigate through a website.²⁴ Once activated, the Meta Pixel "tracks the

²³ <https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>

²⁴ <https://developers.facebook.com/docs/meta-pixel/>

people and type of actions they take.”²⁵ Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information that users input into a website.²⁶

52. For example, if Meta Pixel is incorporated on a shopping website, it may log what searches a user performed, which items of clothing a user clicked on, whether they added an item to their cart, as well as what they purchased. Along with this data, Facebook collects identifying information like IP addresses, Facebook IDs, and other data that allow Facebook to identify the user. Once Facebook receives this information, Facebook processes it, analyzes it, and assimilates it into datasets like its Core Audiences and Custom Audiences.

53. Facebook can then share analytic metrics with the website host, while at the same time sharing the information it collects with third-party advertisers who can then target users based on the information collected and shared by Facebook.

54. Facebook touted Meta Pixel (which it originally called “Facebook Pixel”) as “a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website.”²⁷ According to Facebook, the Meta Pixel is an analytics tool that allows business to measure the effectiveness of their advertising by understanding the actions people take on their websites.”²⁸

55. Facebook warns web developers that its Pixel is a personal identifier because it enables Facebook “to match your website visitors to their respective Facebook User accounts.”²⁹

56. Facebook recommends that its Meta Pixel code be added to the base code on every website page (including the website’s persistent header) to reduce the chance of browsers

²⁵ <https://www.facebook.com/business/goals/retargeting>

²⁶ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

²⁷ <https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/>

²⁸ <https://www.oviond.com/understanding-the-facebook-pixel>

²⁹ <https://developers.facebook.com/docs/meta-pixel/get-started>

or code from blocking Pixel's execution and to ensure that visitors will be tracked.³⁰

57. Once Meta Pixel is installed on a business's website, the Meta Pixel tracks users as they navigate through the website and logs which pages are visited, which buttons are clicked, the specific information entered in forms (including personal information), as well as "optional values" set by the business website.³¹ Meta Pixel tracks this data regardless of whether a user is logged into Facebook.³²

58. For Facebook, the Meta Pixel tool embedded on third-party websites acts as a conduit for information, sending the information it collects to Facebook through scripts running in a user's internet browser, similar to how a "bug" or wiretap can capture audio information. The information is sent in data packets, which include personally identifying data such as a user's IP address.

59. For example, the Meta Pixel is configured to automatically collect "HTTP Headers" and "Pixel-specific data."³³ HTTP headers collect data including "IP addresses, information about the web browser, page location, document, referrer and person using the website."³⁴ Pixel-specific data includes such data as the "Pixel ID and the Facebook Cookie."³⁵

60. Meta Pixel takes the information it harvests and sends it to Facebook with personally identifiable information, such as a user's IP address, name, email, phone number, and specific Facebook ID, which identifies an individual's Facebook user account. Anyone who has access to this Facebook ID can use this identifier to quickly and easily locate, access, and view a user's corresponding Facebook profile. Facebook stores this information on its servers, and, in

³⁰ <https://developers.facebook.com/docs/meta-pixel/get-started>

³¹ <https://developers.facebook.com/docs/meta-pixel/>

³² <https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients>

³³ <https://developers.facebook.com/docs/meta-pixel/>

³⁴ <https://developers.facebook.com/docs/meta-pixel/>

³⁵ <https://developers.facebook.com/docs/meta-pixel/>

some instances, maintains this information for years.³⁶

61. Facebook has a number of ways to uniquely identify the individuals whose data is being forwarded from third-party websites through the Meta Pixel.

62. If a user has a Facebook account, the user data collected is linked to the individual user's Facebook account. For example, if the user is logged into their Facebook account when the user visits a third-party website where the Meta Pixel is installed, many common browsers will attach third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.

63. Alternatively, Facebook can link the data to a user's Facebook account through the "Facebook Cookie."³⁷ The Facebook Cookie is a workaround to recent cookie-blocking applications used to prevent websites from tracking users.³⁸

64. Facebook can also link user data to Facebook accounts through identifying information collected through Meta Pixel through what Facebook calls "Advanced Matching." These are two forms of Advanced Matching: manual matching and automatic matching.³⁹ Manual matching requires the website developer to manually send data to Facebook so that users can be linked to data. Automatic matching allows Meta Pixel to scour the data it receives from third-party websites to search for recognizable fields, including names and email addresses that correspond with users' Facebook accounts.

65. While the Meta Pixel tool "hashes" personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent *Facebook*

³⁶ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

³⁷ <https://clearcode.cc/blog/facebook-first-party-cookie-adtech/>

³⁸ <https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/>

³⁹ <https://www.facebook.com/business/help/611774685654668?id=1205376682832142>

from using the data.⁴⁰ In fact, Facebook explicitly uses the hashed information it gathers to link pixel data to Facebook profiles.⁴¹

66. Facebook also receives personally identifying information in the form of user's unique IP addresses that stay the same as users visit multiple websites. When browsing a third-party website that has embedded Facebook code, a user's unique IP address is forwarded to Facebook by GET requests, which are triggered by Facebook code snippets. The IP address enables Facebook to keep track of the website page visits associated with that address.

67. Facebook also places cookies on visitors' computers. It then uses these cookies to store information about each user. For example, the "c_user" cookie is a unique identifier that identifies a Facebook user's ID. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user has one—and only one—unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

68. The data supplied by the c_user cookie allows Facebook to identify the Facebook account associated with the cookie. One simply needs to log into Facebook, and then type www.facebook.com/#, with the c_user identifier in place of the "#." For example, the c_user cookie for Mark Zuckerberg is 4. Logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

69. Similarly, the "lu" cookie identifies the last Facebook user who logged in using a specific browser. Like IP addresses, cookies are included with each request that a user's browser makes to Facebook's servers. Facebook employs similar cookies such as "datr," "fr," "act," "presence," "spin," "wd," "xs," and "fbp" cookies to track users on websites across the

⁴⁰ <https://www.facebook.com/business/help/611774685654668?id=1205376682832142>

⁴¹ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

internet.⁴² These cookies allow Facebook to easily link the browsing activity of its users to their real-world identities, and such highly sensitive data as medical information, religion, and political preferences.⁴³

70. Facebook also uses browser fingerprinting to uniquely identify individuals. Web browsers have several attributes that vary between users, like the browser software system, plugins that have been installed, fonts that are available on the system, the size of the screen, color depth, and more. Together, these attributes create a fingerprint that is highly distinctive. The likelihood that two browsers have the same fingerprint is at least as low as 1 in 286,777, and the accuracy of the fingerprint increases when combined with cookies and the user's IP address. Facebook recognizes a visitor's browser fingerprint each time a Facebook button is loaded on a third-party website page. Using these various methods, Facebook can identify individual users, watch as they browse third-party websites like www.emersonhospital.org and target users with advertising based on their web activity.

D. Defendant has discretely embedded the Meta Pixel tool on its website, resulting in the capture and disclosure of patients' protected health information to Facebook.

71. A third-party website that incorporates Meta Pixel benefits from the ability to analyze a user's experience and activity on the website to assess the website's functionality and traffic. The third-party website also gains information from its customers through Meta Pixel that can be used to target them with advertisements, as well as to measure the results of advertisement efforts.

72. Facebook's intrusion into the personal data of the visitors to third-party websites incorporating the Meta Pixel is both significant and unprecedented. When Meta Pixel is

⁴² <https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbf8a#:~:text=browser%20session%20ends.-%E2%80%9Cdatr%E2%80%9D,security%20and%20site%20integrity%20features.>

⁴³ https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf

incorporated into a third-party website, unbeknownst to users and without their consent, Facebook gains the ability to surreptitiously gather every user interaction with the website ranging from what the user clicks on to the personal information entered on a website search bar. Facebook aggregates this data against all websites.⁴⁴ Facebook benefits from obtaining this information because it improves its advertising network, including its machine-learning algorithms and its ability to identify and target users with ads.

73. Facebook provides websites using Meta Pixel with the data it captures in the “Meta Pixel page” in Events Manager, as well as tools and analytics to reach these individuals through future Facebook ads.⁴⁵ For example, websites can use this data to create “custom audiences” to target the specific Facebook user, as well as other Facebook users who match “custom audience’s” criteria.⁴⁶ Businesses that use Meta Pixel can also search through Meta Pixel data to find specific types of users to target, such as men over a certain age.

74. Meta Pixel is wildly popular and embedded on millions of websites. Shockingly, Meta Pixel is incorporated on many websites that are used to store and convey sensitive medical information, that by law must be kept private. Recently, investigative journalists have determined that Meta Pixel is embedded on the websites of many of the top hospitals in the United States and on the password-protected portions of many healthcare systems.⁴⁷ This results in sensitive medical information being collected and then sent to Facebook when a user interacts with these hospital websites. For example, when a user on many of these hospital websites clicks on a “Schedule Online” button next to a doctor’s name, Meta Pixel sends the text of the button, the doctor’s name, and the search term (such as “cardiology”) used to find the doctor to

⁴⁴ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

⁴⁵ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

⁴⁶ <https://developers.facebook.com/docs/marketing-api/reference/custom-audience/>

⁴⁷ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

Facebook. If the hospital's website has a drop-down menu to select a medical condition in connection with locating a doctor or making an appointment, that condition is also transmitted to Facebook through Meta Pixel.

75. Facebook has designed the Meta Pixel such that Facebook receives information about patient activities on hospital websites as they occur in real time. Indeed, the moment that a patient takes any action on a webpage that includes the Meta Pixel—such as clicking a button to register, login, logout, or to create an appointment—Facebook code embedded on that page redirects the content of the patient's communications to Facebook while the exchange of information between the patient and hospital is still occurring.

76. Defendant is among the hospital systems who have embedded Meta Pixel on their websites. When a patient enters their personal information through Defendant's websites that incorporate Meta Pixel, such as to locate a doctor or make an appointment, this information, including what the patient is being treated for, those communications are immediately and instantaneously routed to Facebook via the Meta Pixel. The acquisition and disclosure of these communications occurs contemporaneously with the transmission of these communications by patients.

77. This data, which can include health conditions (e.g., addiction, Alzheimer's, heart disease), diagnoses, procedures, test results, the treating physician, medications, and other personally identifying information ("Personal Health Information"), is obtained and used by Facebook, as well as other parties, for the purpose of targeted advertising.

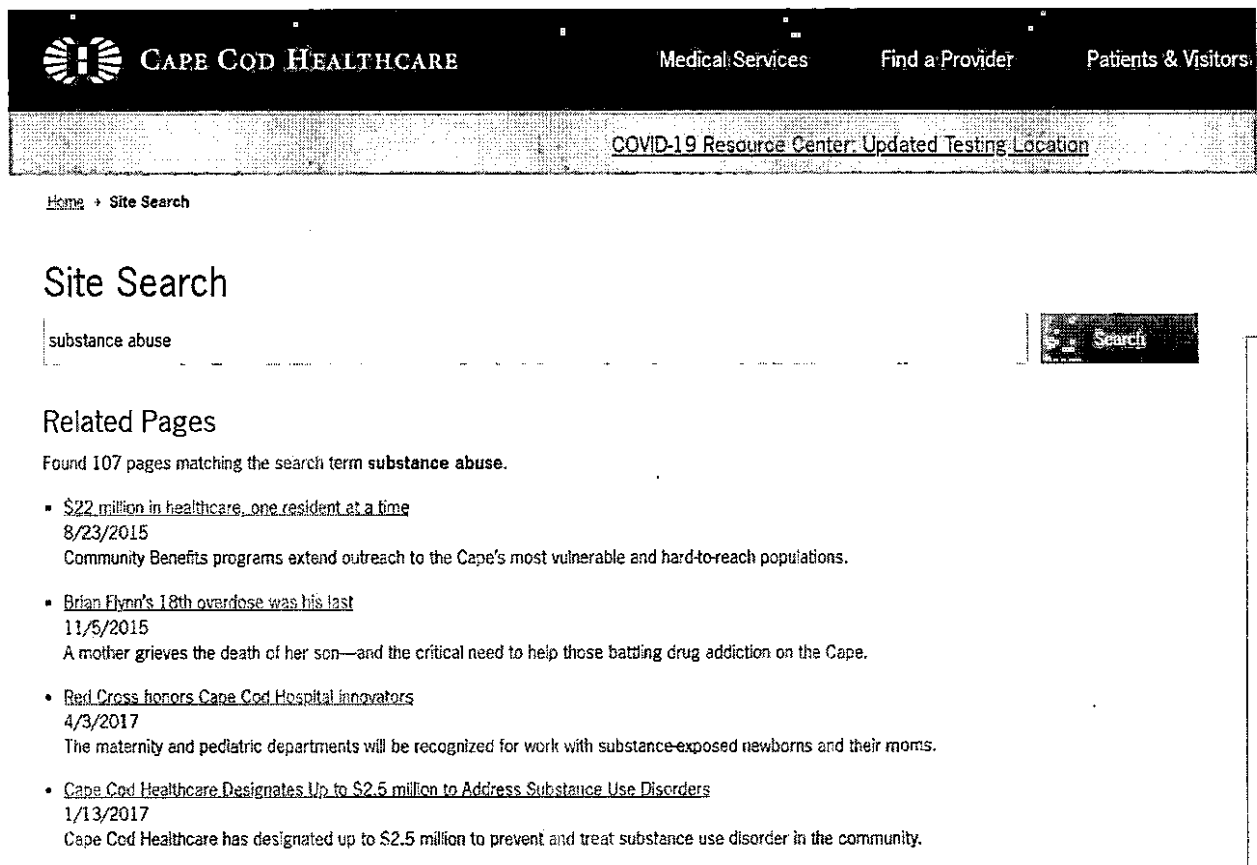
78. For example, a patient searching for a doctor on Defendant's website is asked to provide a variety of information to filter the various physicians available to treat various medical conditions, including the doctor's specialty, the patient's hometown, the patient's language

preference, and other information that the patient provides.

79. The search criteria entered by prospective patients then results in the website providing a list of potential treating physicians who can provide the requested medical services:

80. All this data is disclosed to Facebook simultaneously in real time as patients transmit their information, along with other data, such as patient's unique Facebook ID that is captured by the c_user cookie, which allows Facebook to link this information to patients' unique Facebook accounts. Defendant also discloses other personally identifying information to Facebook, such as patient IP addresses, cookie identifiers, browser-fingerprints, and device identifiers.

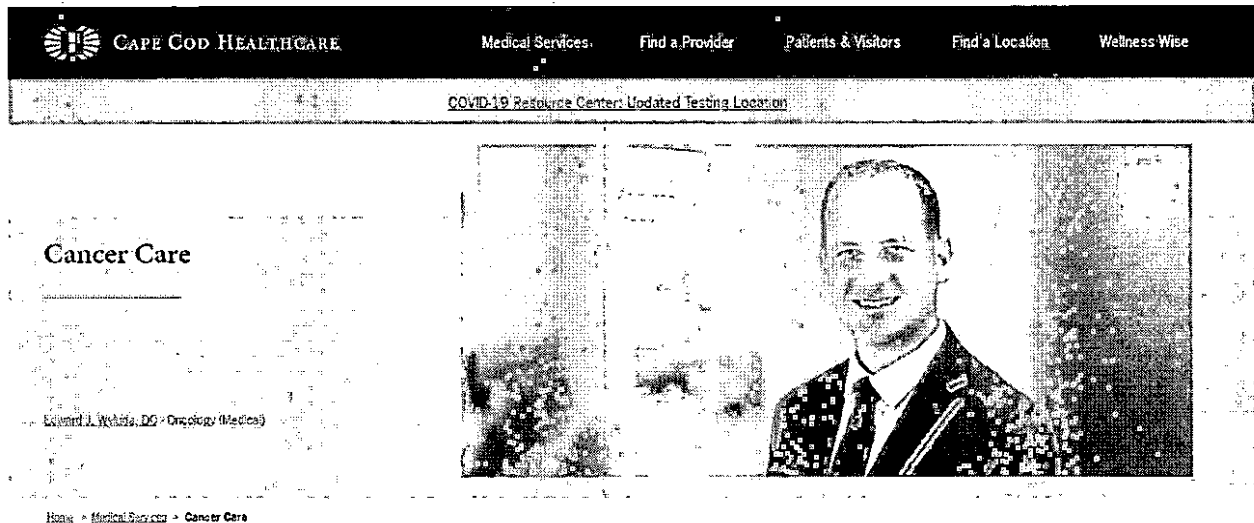
81. Defendant discloses such personally identifying information and sensitive medical information even when patients are searching for doctors to assist with their conditions such as substance abuse and addiction:



The screenshot shows the Cape Cod Healthcare website. The header includes the logo and navigation links: Medical Services, Find a Provider, and Patients & Visitors. A banner for the COVID-19 Resource Center is visible. Below the header, there is a 'Home + Site Search' link. The main content area is titled 'Site Search' and shows a search bar with the text 'substance abuse' and a 'Search' button. Below the search bar, the section 'Related Pages' is displayed, indicating that 107 pages match the search term. The related pages list includes:

- [\\$22 million in healthcare, one resident at a time](#)
8/23/2015
Community Benefits programs extend outreach to the Cape's most vulnerable and hard-to-reach populations.
- [Brian Flynn's 18th overdose was his last](#)
11/5/2015
A mother grieves the death of her son—and the critical need to help those battling drug addiction on the Cape.
- [Red Cross honors Cape Cod Hospital innovators](#)
4/3/2017
The maternity and pediatric departments will be recognized for work with substance-exposed newborns and their moms.
- [Cape Cod Healthcare Designates Up to \\$2.5 million to Address Substance Use Disorders](#)
1/13/2017
Cape Cod Healthcare has designated up to \$2.5 million to prevent and treat substance use disorder in the community.

82. Likewise, a patient who searches the website for information about receiving certain specific forms of medical treatment such as orthopedics, heart & vascular care, or cancer care also has information about their queries and the specific web pages that the patient has visited acquired by Defendant and forwarded to Facebook:



83. Defendant also discloses patient information from other sections of its website including (but not limited to) communications that are captured by the website's search bar, communications that are captured when a patient searches for "Medical Services" offered by Defendant, communications made by patients using the website's Bill Pay/Financials function, and communications made when patients are researching specific medical conditions such as COVID-19.

84. By compelling visitors to its websites to disclose personally identifying data and sensitive medical information to Facebook and other third parties, Defendant knowingly discloses information that allows Facebook and other advertisers to link its patients' Personal Health Information to their private identities and target them with advertising. Defendant intentionally shares the Personal Health Information of its patients with Facebook in order to

gain access to the benefits of the Meta Pixel tool.

85. Defendant facilitated the disclosure of Plaintiff Jane Doe's Personal Health information, including sensitive medical information, to Facebook without her consent or authorization when she entered information on the website that Defendant maintains at www.capecodhealth.org. Plaintiff continued to have her privacy violated when Defendant permitted Facebook and other companies to send her targeted advertising related to her medical condition.

86. For example, Plaintiff Jane Doe visited Defendant's website in 2021 at www.capecodhealth.org and entered data, including sensitive medical information, such as details about her medical condition and doctor. The information that Plaintiff Jane Doe transmitted included queries about treatment for skin cancer. Plaintiff Jane Doe believed that her interactions with Defendant's website were private and would not be shared with anyone besides her health care providers and their staff. Plaintiff Jane Doe was surprised and dismayed when she learned that her Personal Health Information, including private and potentially embarrassing facts, had been sent to Facebook without her consent.

87. Defendant knew that by embedding Meta Pixel—a Facebook advertising tool—it was permitting Facebook to collect, use, and share Plaintiff's and the Class Members' Personal Health Information, including sensitive medical information and personally identifying data. Defendant was also aware that such information would be shared with Facebook simultaneously with patients' interactions with its websites. Defendant made the decision to barter its patients' Personal Healthcare Information to Facebook because it wanted access to the Meta Pixel tool. While that bargain may have benefited Defendant and Facebook, it also betrayed the privacy rights of Plaintiff and Class Members.

F. Plaintiff and the Class Members did not consent to the interception and disclosure of their protected health information.

88. Plaintiff and Class Members had no idea when they interacted with Defendant's websites that their personal data, including sensitive medical data, was being collected and simultaneously transmitted to Facebook. That is because, among other things, Meta Pixel is seamlessly integrated into Defendant's websites and is invisible to patients visiting those websites.

89. For example, when Plaintiff Jane Doe visited Defendant's website in 2021 at www.capecodhealth.org, there was no indication that Meta Pixel was embedded on that website or that it would collect and transmit her sensitive medical data to Facebook.

90. Plaintiff and her fellow Class Members could not consent to Defendant's conduct when there was no indication that their sensitive medical information would be collected and transmitted to Facebook in the first place.

91. While Defendant purports to have a "Privacy Policy," that Privacy Policy is effectively hidden from patients. Unlike most hospital websites, the home page of Defendant's website contains no link to its online Privacy Policy.⁴⁸ Instead, the only way that a visitor to Defendant's website could even locate the Privacy Policy is by entering the term "Privacy" or something similar in the website's search bar and engaging the search function.

92. Defendant's "Privacy Policy" gives no indication to patients that Defendant routinely allows Facebook to capture and exploit patients' Personal Health Information. Indeed, Defendant expressly promises in its "Privacy Policy" that it would safeguard both the identifies and the personal health information provided by visitors to its website⁴⁹:

⁴⁸ <https://www.capecodhealth.org/>

⁴⁹ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

Privacy Policy

Cape Cod Healthcare's Internet Privacy Policy

At Cape Cod Healthcare, we are committed to protecting the privacy and security of the users of our Internet site. We understand that one's health is often a very personal, private subject, and, accordingly, we are committed to protecting the identities of visitors to our site. This Privacy Policy will tell you what information we collect, how it is used, and what your choices are. Please read this policy carefully.

93. Even if a patient stumbled upon Defendant's carefully hidden "Privacy Policy," nothing in that notice would be understood by any reasonable patient to mean that Defendant is routinely allowing Facebook to capture and exploit patients' Personal Health Information.

94. While disclosing that its website contains "cookies," Defendant's Privacy Policy falsely promises that the information Defendant collects "do not contain any personally identifiable information."⁵⁰ Contrary to that promise, Defendant's website automatically transmits personally identifiable information to Facebook using multiple cookies, including the c_user, datr, fr, sb, and xs cookies.

95. Defendant does not have a legal right to share Plaintiff and Class Members' Protected Health Information with Facebook, because this information is protected from such disclosure by law. *E.g.* GL c. 214, §1B; 45 C.F.R. § 164.508. Moreover, Defendant is not permitted to disclose patients' Protected Health Information to an advertising and marketing company like Facebook without express written authorization from patients. . *E.g.* 940 Mass. Code Regs. 4.08(12).

96. Defendant failed to obtain a valid written authorization from Plaintiff or any of the Class Members to allow the capture and exploitation of their personally identifiable information and the contents of their communications for marketing purposes.

97. A patient's reasonable expectation that their health care provider will not share their information with third parties for marketing purposes is not subject to waiver via an

⁵⁰ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

inconspicuous privacy policy hidden away on a company's website. Such "Browser-Wrap" statements do not create an enforceable contract against consumers. Further, Defendant expressly promised its patients that it would never sell or use their Personal Health Information for marketing purposes without express authorization.

98. Accordingly, Defendant lacked authorization to intercept, collect, and disclose Plaintiff and Class Members' Personal Health Information to Facebook or aid in the same.

G. The disclosures of personal patient data to Facebook are unnecessary.

99. There is no information anywhere on the websites operated by Defendant that would alert patients that their most private information (such as their identifiers, their medical conditions, and their medical providers) is being automatically transmitted to Facebook. Nor are any of the disclosures of patient Personal Health Information to Facebook necessary for Defendant to maintain its healthcare website or provide medical services to patients.

100. For example, it is possible for a healthcare website to provide a doctor search function without allowing disclosures to third-party advertising companies about patient sign ups or appointments. It is also possible for a website developer to utilize tracking tools without allowing disclosure of patients' Personal Healthcare Information to companies like Facebook. Likewise, it is possible for Defendant to provide medical services to patients without sharing their Personal Health Information with Facebook so that this information can be exploited for advertising purposes.

101. Despite these possibilities, Defendant willfully chose to implement Meta Pixel on its websites and aid in the disclosure of personally identifiable information and sensitive medical information about its patients, as well as the contents of their communications with Defendant, to third-parties, including Facebook.

H. Plaintiff and Class Members have a reasonable expectation of privacy in their Personal Health Information, especially with respect to sensitive medical information.

102. Patient confidentiality “is a cardinal rule of the medical profession, faithfully adhered to in most instances, and thus has come to be justifiably relied upon by patients seeking advice and treatment.” *Alberts v. Devine*, 395 Mass. 59, 65 (1985).

103. Plaintiff and Class Members have a reasonable expectation of privacy in their Personal Health Information, including personally identifying data and sensitive medical information. Defendant’s surreptitious interception, collection, and disclosure of patients’ Personal Health Information to Facebook violated Plaintiff and Class Member’s privacy interests.

104. Patient health information is specifically protected by law. *E.g.* G.L. 111, §70E(b); G.L. 214, §1B. The prohibitions against disclosing patient Personal Health Information include prohibitions against disclosing personally identifying data such patient names, IP addresses, and other unique characteristics or codes. *E.g.* 105 Mass. Code Regs. 300.120; 45 C.F.R. § 164.514. And Massachusetts law subject medical providers who treat conditions such as substance abuse to heightened duties of confidentiality. G.L. c. 111B, § 11. This legal framework applies to health care providers, such as Defendant.

105. Given the public policy expressed by these laws, coupled with Defendant’s express promises that it would protect the confidentiality of Plaintiff’s and Class Members’ Personal Health Information, Plaintiff and the Members of the Class had a reasonable expectation of privacy in their protected health information.

106. Several studies examining the collection and disclosure of consumers’ sensitive medical information confirm that the disclosure of sensitive medical information violates expectations of privacy that have been established as general social norms.

107. Privacy polls and studies also uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

108. For example, a recent study by *Consumer Reports* showed that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believed that internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.⁵¹

109. Users act consistently with these preferences. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to share data when prompted.⁵²

110. The concern about sharing personal medical information is compounded by the reality that advertisers view this type of information as particularly valuable. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one recent article noted, “What is particularly worrying about this process of datafication of children is that companies like [Facebook] are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles.”⁵³

111. Many privacy law experts have expressed serious concerns about patients' sensitive medical information being disclosed to third-party companies like Facebook. As those

⁵¹ <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/>

⁵² <https://www.wired.co.uk/article/apple-ios14-facebook>

⁵³ <https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/>

critics have pointed out, having a patient's personal health information disseminated in ways the patient is unaware of could have serious repercussions, including affecting their ability to obtain life insurance, how much they might pay for such coverage, the rates they might be charged on loans, and the likelihood of their being discriminated against.

I. Plaintiff's Personal Health Data that Defendant collected, disclosed, and used is Plaintiff's property, has economic value, and its illicit disclosure has caused Plaintiff harm.

112. It is common knowledge that there is an economic market for consumers' personal data—including the kind of data that Defendant has collected and disclosed from Plaintiff and Class Members.

113. In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, “age, gender and location information” were being sold for approximately “\$0.50 per 1,000 people.”⁵⁴

114. In 2015, *TechCrunch* reported that “to obtain a list containing the names of individuals suffering from a particular disease,” a market participant would have to spend about “\$0.30” per name.⁵⁵ That same article noted that “Data has become a strategic asset that allows companies to acquire or maintain a competitive edge” and that the value of a single user's data can vary from \$15 to more than \$40 per user.⁵⁶

115. In a 2021 Washington Post article, the legal scholar Dina Srinivasan said that consumers “should think of Facebook's cost as [their] data and scrutinize the power it has to set its own price.”⁵⁷ This price is only increasing. According to Facebook's own financial statements, the value of the average American's data in advertising sales rose from \$19 to \$164

⁵⁴ <https://ig.ft.com/how-much-is-your-personal-data-worth/>

⁵⁵ <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>

⁵⁶ <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>

⁵⁷ <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/>

per year between 2013 and 2020.⁵⁸

116. Despite the protections afforded by law, there is an active market for health information. Medical information obtained from health providers garners substantial value because of the fact that it is not generally available to third party data marketing companies because of the strict restrictions on disclosure of such information by state laws and provider standards, including the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for the sale and purchase of such private medical information.⁵⁹

117. Further, individuals can sell or monetize their own data if they so choose. For example, Facebook has offered to pay individuals for their voice recordings,⁶⁰ and has paid teenagers and adults up to \$20 a month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smart phones.⁶¹

118. A myriad of other companies and apps such as DataCoup, Nielsen Computer, Killi, and UpVoice also offer consumers money in exchange for access to their personal data.⁶²

119. Given the monetary value that data companies like Facebook have already paid for personal information in the past, Defendant has deprived Plaintiff and the Class Members of the economic value of their sensitive medical information by collecting, using, and disclosing that information to Facebook and other third parties without consideration for Plaintiff and the Class Member's property.

J. Defendant is enriched by making unlawful, unauthorized, and unnecessary disclosures of its patients' protected health information.

⁵⁸ <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/>

⁵⁹ <https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it/>; *see also* <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>

⁶⁰ <https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-pronunciations-app>

⁶¹ <https://www.cnb.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html>

⁶² <https://www.creditdonkey.com/best-apps-data-collection.html>; *see also* <https://www.monetha.io/blog/rewards/earn-money-from-your-data/>

120. In exchange for disclosing Personal Health Information about its patients, Defendant is compensated by Facebook with enhanced online advertising services, including (but not limited to) retargeting and enhanced analytics functions.

121. Retargeting is a form of online targeted advertising that targets users with ads based on their previous internet actions, which is facilitated through the use of cookies and tracking pixels. Once an individual's data is disclosed and shared with a third-party marketing company, the advertiser is able to show ads to the user elsewhere on the internet.

122. For example, retargeting could allow a web-developer to show advertisements on other websites to customers or potential customers based on the specific communications exchanged by a patient or their activities on a website. Using the Meta Pixel, a website could target ads on Facebook itself or on the Facebook advertising network. The same or similar advertising can be accomplished via disclosures to other third-party advertisers and marketers.

123. Once personally identifiable information relating to patient communications is disclosed to third parties like Facebook, Defendant loses the ability to control how that information is subsequently disseminated and exploited.

124. The monetization of the data being disclosed by Defendant, both by Defendant and Facebook, demonstrates the inherent value of the information being collected.

K. Facebook's history of egregious privacy violations.

125. Defendant knew or should have known that Facebook could not be trusted with its patients' sensitive medical information.

126. Due to its ability to target individuals based on granular data, Facebook's ad-targeting capabilities have frequently come under scrutiny. For example, in June 2022, Facebook entered into a settlement with the Department of Justice regarding its Lookalike Ad

service, which permitted targeted advertising by landlords based on race and other demographics in a discriminatory manner. That settlement, however, reflected only the latest in a long history of egregious privacy violations by Facebook.

127. In 2007, when Facebook launched “Facebook Beacon,” users were unaware that their online activity was tracked, and that the privacy settings originally did not allow users to opt-out. As a result of widespread criticism, Facebook Beacon was eventually shut down.

128. Two years later, Facebook made modifications to its Terms of Service, which allowed Facebook to use anything a user uploaded to its site for any purpose, at any time, even after the user ceased using Facebook. The Terms of Service also failed to provide for any way for users to completely delete their accounts. Under immense public pressure, Facebook eventually returned to its prior Terms of Service.

129. In 2011, Facebook settled charges with the Federal Trade Commission relating to its sharing of Facebook user information with advertisers, as well as its false claim that third-party apps were able to access only the data they needed to operate when—in fact—the apps could access nearly all of a Facebook user’s personal data. The resulting Consent Order prohibited Facebook from misrepresenting the extent to which consumers can control the privacy of their information, the steps that consumers must take to implement such controls, and the extent to which Facebook makes user information available to third parties.⁶³

130. Facebook found itself in another privacy scandal in 2015 when it was revealed that Facebook could not keep track of how many developers were using previously downloaded Facebook user data. That same year, it was also revealed that Facebook had violated users’ privacy rights by harvesting and storing Illinois’ users’ facial data from photos without asking for their consent or providing notice. Facebook ultimately settled claims related to this unlawful

⁶³ <https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter>

act for \$650 million.⁶⁴

131. In 2018, Facebook was again in the spotlight for failing to protect users' privacy. Facebook representatives testified before Congress that a company called Cambridge Analytics may have harvested the data of up to 87 million users in connection with the 2016 election. This led to another FTC investigation in 2019 into Facebook's data collection and privacy practices, resulting in a record-breaking five-billion-dollar settlement.

132. Likewise, a different 2018 report revealed that Facebook had violated users' privacy by granting access to user information to over 150 companies.⁶⁵ Some companies were even able to read users' private messages.

133. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.⁶⁶ This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

134. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective ... at preventing the

⁶⁴ A similar case is pending in Texas.

⁶⁵ <https://www.cnn.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html>

⁶⁶ <https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/>

receipt of sensitive data.”⁶⁷

135. The New York State Department of Financial Service’s concern about Facebook’s cavalier treatment of private medical data is not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook’s monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.⁶⁸ When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo “took no action to limit what these companies could do with users’ information.”⁶⁹

136. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that “We do not have an adequate level of control and explainability over how our systems use data, and thus we can’t confidently make controlled policy changes or external commitments such as ‘we will not use X data for Y purpose.’”⁷⁰

137. These revelations were confirmed by an article published by the Markup on June 16, 2022, which found during the course of its investigation that Facebook’s purported “filtering” failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites

⁶⁷ https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf

⁶⁸ <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>

⁶⁹ <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>

⁷⁰ <https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes>

not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.⁷¹

138. Despite knowing that the Meta Pixel code embedded in its websites was sending patients' Personal Health Information to Facebook, Defendant did nothing to protect its patients from egregious intrusions into its patients' privacy, choosing instead to benefit at those patients' expense.

TOLLING, CONCEALMENT, AND ESTOPPEL

139. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

140. Defendant seamlessly incorporated Meta Pixel and other trackers into its websites, providing no indication to users that they were interacting with a website enabled by Meta Pixel. Defendant had knowledge that its websites incorporated Meta Pixel and other trackers yet failed to disclose that by interacting with Meta-Pixel enabled websites that Plaintiff and Class Members' sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook.

141. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendants' conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel.

142. The earliest that Plaintiff and Class Members, acting with due diligence, could have reasonably discovered this conduct would have been on June 16, 2022, following the release of the Markup's investigation.

⁷¹ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

143. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Defendant's illegal interception and disclosure of patients' Personal Health Information has continued unabated through the date of the filing of Plaintiff's Original Complaint. What's more, Defendant was under a duty to disclose the nature and significance of their data collection practices but did not do so. Defendant is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

144. Defendant's conduct violates the law and breaches its express and implied privacy promises.

145. Defendant's unlawful conduct has injured Plaintiff and Class Members.

146. Defendant's conduct is ongoing.

147. Plaintiff brings this action individually and as a class action against Defendant.

148. Plaintiff seeks class certification for the following proposed Class:

The Cape Cod Healthcare Class: During the fullest period allowed by law, all Massachusetts residents who are, or were, patients of Cape Cod Healthcare or any of its affiliates and who exchanged communications at Cape Cod Healthcare's websites, including www.capecodhealth.org and any other Cape Cod Healthcare hospital affiliated website that caused disclosures of patient personally identifiable information and communications to third parties, including (but not limited to) Facebook.

149. Excluded from the proposed Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) the Defendant, Defendant's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendant or its parent has a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendant's counsel.

150. Plaintiff reserves the right to redefine the Class and/or add Subclasses at, or prior

to, the class certification stage, in response to discovery or pursuant to instruction by the Court.

151. This action is properly maintainable as a class action as specifically defined in Massachusetts Rule of Civil Procedure 23.

152. **Numerosity:** While the exact number of Class Members is unknown to Plaintiff at this time, the Class, based on information and belief, consists of thousands of people dispersed throughout the Commonwealth of Massachusetts, such that joinder of all members is impracticable. The exact number of Class Members can be determined by review of information maintained by Defendants.

153. **Commonality and Predominance:** There are questions of law and fact common to Class Members and which predominate over any questions affecting only individual members. A class action will generate common answers to the questions below, which are apt to drive resolution:

- a. Whether Defendant's acts and practices violated Plaintiff and Class Members' privacy rights;
- b. Whether Defendant's acts and practices violate G.L. c. 272, § 99;
- c. Whether Defendant's acts and practices violate G.L. c. 214, § 1B;
- d. Whether Defendant's acts and practices violate G.L. c. 111, § 70E;
- e. Whether Defendant knowingly allowed the surreptitious collection and disclosure of Plaintiff and Class Members' Personal Health Information to Facebook;
- f. Whether Defendant's acts and practices constitute a breach of fiduciary duty;
- g. Whether Defendant profited from disclosures of patient Personal Health Information to third parties including Facebook;
- h. Whether Defendant was unjustly enriched;
- i. Whether Defendant's acts and practices harmed and continue to harm Plaintiff and Class Members and, if so, the extent of that injury;
- j. Whether Plaintiff and Class Members are entitled to equitable relief including, but not limited to, injunctive relief, restitution, and disgorgement; and

- k. Whether Plaintiff and Class Members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

154. These common questions of law and fact predominate over any questions affecting only the individual Class Members.

155. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

156. **Typicality:** Plaintiff's claims are typical of the claims of other Class Members and Plaintiff have substantially the same interest in this matter as other Class Members. Plaintiff has no interests that are antagonist to, or in conflict with, the interests of other members of the Class. Plaintiff's claims arise out of the same set of facts and conduct as all other Class Members. Plaintiff and all Class Members are patients of Defendant who used the websites set up by Defendant for patients and are victims of Defendant's respective unauthorized disclosures to third parties including Facebook. All claims of Plaintiff and Class Members are based on Defendant's wrongful conduct and unauthorized disclosures.

157. **Adequacy of Representation:** Plaintiff is committed to prosecuting this action and has retained competent counsel experienced in litigation of this nature. Plaintiff's claims are coincident with, and not antagonistic to, those of other Class Members he seeks to represent. Plaintiff has no disabling conflicts with Class Members. Accordingly, Plaintiff is an adequate representative of the Class and, along with counsel, will fairly and adequately protect the interests of the Class and any Subclasses.

158. **Superiority:** A class action is the superior method for fair and efficient adjudication of the controversy. Although all Class Members have claims against Defendant, the likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to conduct such litigation. The damages, harm, and other detriment suffered individually by Plaintiff and other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impractical for Class Members to individually seek redress for Defendant's wrongful conduct. Moreover, serial adjudication in numerous venues is not efficient, timely, or proper. Judicial resources would be unnecessarily depleted by prosecution of individual claims. The prosecution of separate actions by individual Class Members could create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which could establish incompatible standards of conduct for Defendant or adjudications with respect to individual members of the Class which would, as a practical matter, be dispositive of the interests of the members of the Class Members who are not parties to the adjudications. If a class action is not permitted, Class Members will continue to suffer losses and Defendant's misconduct will continue without proper remedy.

159. Plaintiff anticipates no unusual difficulties in the management of this litigation as a class action. The Class is readily ascertainable and direct notice can be provided from the records maintained by Defendant, electronically or by publication, the cost of which is properly imposed on Defendant.

160. For the above reasons, among others, a class action is superior to other available methods for the fair and efficient adjudication of this action.

CAUSES OF ACTION

COUNT I

**Interception of Wire Communications in Violation of
G.L. c. 272, § 99
(On Behalf of Plaintiff and the Class)**

161. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

162. Plaintiff brings this claim on behalf of herself and all members of the Class.

163. All conditions precedent to this action have been performed or have occurred.

164. G.L. c. 272, § 99 prohibits any person from willfully and secretly intercepting the contents of any wire communications through the use of any intercepting device unless given prior authority by all parties to a communication to do so.

165. Any person aggrieved by a violation G.L. c. 272, § 99 “shall have a civil cause of action against any person who so intercepts, discloses, or uses such communications or who so violates his personal, property, or privacy interest.”

166. Defendant qualifies as a person under the statute.

167. All alleged communications between Plaintiff or Class Members and Defendant qualify as wire communications under Massachusetts law because each communication is made using personal computing devices (e.g., computers, smartphones, tablets) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

168. An “interception” under the statute means “to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire ... communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication.” G.L. c. 272, § 99B(4).

169. Defendant engaged in and continues to engage in an “interception” by aiding others (including Facebook) to secretly record the contents of Plaintiff’s and Class Members’ wire communications.

170. An “intercepting device” is “any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire ... communication.” G.L. c. 272, § 99B(3).

171. The “intercepting devices” used in this case include, but are not limited to:

- a. Plaintiff and Class Members’ personal computing devices;
- b. Plaintiff and Class Members’ web browsers;
- c. Plaintiff and Class Members’ browser-managed files;
- d. Facebook’s Meta Pixel;
- e. Internet cookies;
- f. Defendant’s computer servers;
- g. Third-party source code utilized by Defendant; and
- h. Computer servers of third parties (including Facebook) to which Plaintiff and Class Members’ communications were disclosed.

172. Under the statute, “contents” are defined to mean “any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication.” G.L. c. 272, § 99B(5).

173. Defendant aided in, and continues to aid in, the interception of contents in that the data from the communications between Plaintiff and/or Class Members and Defendant that were redirected to and recorded by the third parties include information which identifies the parties to each communication, their existence, and their contents.

174. Defendant aided in the interception of “contents” in at least the following forms:

- a. The parties to the communications;
- b. The precise text of patient search queries;
- c. Personally identifying information such as patients’ IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;
- d. The precise text of patient communications about specific doctors;
- e. The precise text of patient communications about specific medical conditions;
- f. The precise text of patient communications about specific treatments;
- g. The precise text of patient communications about scheduling appointments with medical providers;
- h. The precise text of patient communications about billing and payment;
- i. The precise text of specific buttons on Defendant’s website(s) that patients click to exchange communications, including Log-Ins, Registrations, Requests for Appointments, Search; and other buttons;
- j. The precise dates and times when patients click to Log-In on Defendant’s website(s);
- k. Information that is a general summary or informs third parties of the general subject of communications that Defendant sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information; and
- l. Any other content that Defendant has aided third parties in scraping from webpages or communication forms at web properties.

175. Plaintiff and Class Members reasonably expected that their Personal Health Information was not being intercepted, recorded, and disclosed to Facebook and other third parties.

176. No legitimate commercial purpose was served by Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Personal Health Information to Facebook. Neither Plaintiff nor Class Members consented to the disclosure of their Personal Health Information by Defendant to Facebook and other third parties. Nor could they have consented, given that Defendant never sought Plaintiff or Class Members' consent., much less told visitors to its website that their every interaction was being recorded and transmitted to Facebook via the Meta Pixel tool.

177. Plaintiff and Class Members' electronic communications were intercepted during transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their Personal Health Information, including using their sensitive medical information to develop marketing and advertising strategies.

178. Under the statute, aggrieved persons are entitled to recover appropriate injunctive relief and "(1) actual damages but not less than liquidated damages computed at the rate of \$100 per day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) a reasonable attorney's fee and other litigation disbursements reasonably incurred."

179. In addition to statutory damages, Defendant's breach caused Plaintiff and Class Members the following damages:

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- b. Defendant eroded the essential confidential nature of the doctor-patient relationship;

- c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and
- e. Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

COUNT II
Invasion of Privacy in Violation of G.L. c. 214, § 1B
(On Behalf of Plaintiff and the Class)

180. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

181. Plaintiff bring this claim on behalf of herself and all members of the Class.

182. G.L. c. 214, § 1B provides that "a person shall have a right against unreasonable, substantial, or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages."

183. All health care providers owe their patients a duty not to disclose medical information about a patient without a patient's informed consent.

184. G.L. c. 111, § 70E provides that every patient or resident of a Massachusetts health care facility shall have the right to "confidentiality of all records and communications to the extent provided by law."

185. Maintaining the confidentiality of the doctor-patient relationship is a cardinal rule of the medical profession which has come to be justifiably relied on by patients seeking advice and treatments.

186. Plaintiff and Class Members are patients of Defendant.

187. Defendant owes Plaintiff and Class Members a duty of confidentiality.

188. Despite its duty not to disclose Personal Health Information without informed consent and written authorization, Defendant disclosed information relating to Plaintiff and Class Members' medical treatment to third parties without their knowledge, consent, or authorization.

189. The information disclosed included personally identifiable information, Plaintiff and Class Members' statuses as patients of Defendant, and the exact contents of communications exchanged between Plaintiff and/or Class Members with Defendant, including but not limited to information about treating doctors, potential doctors, conditions, treatments, appointments, search terms, bill payment, and logins to Defendant's website.

190. The disclosure of personally identifiable medical information constitutes an unreasonable, substantial, and serious interference with Plaintiff and Class Members' rights to privacy.

191. Plaintiff and Class Members did not consent to, authorize, or know about Defendant's disclosure of their Personal Health Information to Facebook and other third parties at the time it occurred. Plaintiff and Class Members never agreed that their sensitive medical information could be collected, used, and monetized by Facebook.

192. Defendant's intentional disclosure of patients' Personal Health Information to a third-party advertising company like Facebook without consent would be highly offensive to a reasonable person. Plaintiff and Class Members reasonably expected that their Personal Health Information would not be collected, used, and monetized by third party advertising companies.

193. Defendant's disclosure of Personal Health Information from thousands of individuals was highly offensive because it violated expectations of privacy that have been established by social norms. Privacy polls and studies show that Americans believe that one of

the most important privacy rights is the need for an individual's affirmative consent before their personal data is collected, shared, or used.

194. Given the nature of the Personal Health Information that Defendant disclosed to Facebook, such as patients' names, email addresses, phone numbers, information entered into forms, doctor's names, potential doctor's names, the search terms used to locate doctors (i.e. "Alzheimer's"), the condition selected from dropdown menus (i.e. "Heart Disease"), medications, and details about upcoming doctor's appointments, this kind of intrusion would be (and in fact is) highly offensive to a reasonable person.

195. Defendant's breach caused Plaintiff and Class Members, at minimum, the following damages:

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- b. Defendants eroded the essential confidential nature of the doctor-patient and provider-patient relationship;
- c. Defendants took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff and Class Members' knowledge, consent, or authorization and without sharing the benefit of such value;
- d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain the confidentiality of their Personal Health Information; and
- e. Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

196. Plaintiff and Class Members have suffered harm and injury, including but not limited to the invasion of their privacy rights.

197. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to seek just compensation, including monetary damages.

198. Plaintiff and Class Members seek appropriate relief for their injuries, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as well as a disgorgement of profits made by Defendant as a result of its intrusions on Plaintiff and Class Members' privacy.

199. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, which caused injury to Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

200. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT III

Breach of Fiduciary Duty and/or Common Law Duty of Confidentiality (On Behalf of Plaintiff and the Class)

201. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

202. Plaintiff brings this claim on behalf of herself and all members of the Class.

203. All conditions precedent to this action have been performed or occurred.

204. In *Alberts v. Devine*, 479 N.E.2d 113, 120 (1985), the Massachusetts Supreme Court held that a duty of confidentiality arises from the physician-patient relationship and that a violation of that duty gives rise to a cause of action sounding in tort.

205. As medical provider for Plaintiff and Class Members, Defendant owes Plaintiff and Class Members a fiduciary duty of confidentiality in the data and content of communications exchanged between Defendant and Plaintiff or Class Members.

206. Defendant breached its duty of confidentiality by disclosing Personal Health Information about Plaintiff and Class Members, including their status as patients, the content of their communications, and information about their doctors, potential doctors, conditions, treatments, appointments, search terms, and bill payment.

207. Defendant's breach caused Plaintiff and Class Members the following damages:

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- b. Defendants eroded the essential confidential nature of the doctor-patient and provider-patient relationship;
- c. Defendants took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff and Class Members' knowledge, consent, or authorization and without sharing the benefit of such value;
- d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain the confidentiality of their Personal Health Information; and
- e. Defendant's actions diminished the value of Plaintiff and Class Members' personal information.

COUNT IV
Breach of Express Contract
(On Behalf of Plaintiff and the Class)

208. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

209. Plaintiff bring this claim on behalf of herself and all members of the Class.

210. Plaintiff and Class Members entered into written agreements with Defendant as part of the medical services Defendant provided to Plaintiff and Class Members. The agreements involved a mutual exchange of consideration whereby Defendant provided these services in exchange for payment from Class Members, Class Members' insurance carriers, and/or government programs remitting payment on Class Members' behalf.

211. Plaintiff and Class Members and/or their insurance carriers paid Defendant for its services and performed under these agreements.

212. Defendant's disclosure of Plaintiff and Class Members' Private Health Information without their consent constitutes a material breach of the terms of these agreements by Defendant.

213. As a direct and proximate result of Defendant's breach of contract with Plaintiff and Class Members, Plaintiff and Class Members have been irreparably harmed.

214. Accordingly, Plaintiff, individually and on behalf of the Class, respectfully request this Court award all available damages for Defendant's breach of express contract.

COUNT V
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

215. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

216. Plaintiff brings this claim on behalf of herself and all members of the Class.

217. Defendant promises in its Privacy Policy that it is committed to protecting patients' sensitive medical and personal information, telling patients that "we are committed to protecting the privacy and security of the users of our Internet site."⁷² Defendant assures patients that the information it collects about patients does not include any "personally identifiable information."⁷³ Defendant also promises that "Cape Cod Healthcare wants your personal information to remain as secure as possible. Accordingly, we prevent unauthorized access by a secure firewall and through our use of a security infrastructure to protect the integrity and privacy of the personal information you provide to us."⁷⁴

218. Defendant solicited and invited Plaintiff and Class Members to provide their Private Health Information on its website as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Health Information to Defendant as part of acquiring Defendant's medical services. Per its contractual, legal, ethical, and fiduciary duties, Defendant was obligated to take adequate measures to protect Plaintiff's and Class Members' Personal Health Information from unauthorized disclosure to third parties such as Facebook. These facts give rise to the inference that Defendant took on obligations outside the plain terms of any express contracts that they may have had with Plaintiff and Class Members.

219. Plaintiff and the Class Members entered into valid and enforceable implied contracts with Defendant when they sought medical treatment from Defendant. Specifically, through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of medical care and treatment, which included an implied agreement

⁷² <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

⁷³ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

⁷⁴ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

for Defendant to retain and protect the privacy of Plaintiff's and Class Members' Personal Health Information.

220. Defendant required and obtained Plaintiff's and Class Members' Personal Health Information as part of the physician-patient relationship, evincing an implicit promise by Defendant to act reasonably to protect the confidentiality of Plaintiff's and Class Members' Personal Health Information. Defendant, through its privacy policies, codes of conduct, company security practices, and other conduct, implicitly that it would safeguard Plaintiff's and Class Members' Personal Health Information in exchange for access to that information and the opportunity to treat Plaintiff and Class Members.

221. Implied in the exchange was a promise by Defendant to ensure that the Personal Health Information of Plaintiff and Class Members in its possession would only be used for medical treatment purposes and would not be shared with third parties such as Facebook without the knowledge or consent of Plaintiff and Class Members. By asking for and obtaining Plaintiff's and Class Members' Personal Health Information, Defendant assented to protecting the confidentiality of that information. Defendant's implicit agreement to safeguard the confidentiality of Plaintiff's and Class Members' Personal Health Information was necessary to effectuate the contract between the parties.

222. Plaintiff and Class Members provided their Personal Health Information in reliance on Defendant's implied promise that this information would be safeguarded and not disclosed to third parties without their consent.

223. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class Members would provide their Personal Health Information in exchange for the medical treatment and other benefits provided by Defendant (including the

protection of their confidential personal and medical information). A portion of the price of each payment that Plaintiff and the Class Members made to Defendant for medical services was intended to ensure the confidentiality of their Personal Health Information.

224. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant would comply with its promises to protect the confidentiality of their Personal Health Information as well as applicable laws and regulations governing the disclosure of such information and that Defendant would not allow third parties to collect or exploit their communications with Defendant without their consent.

225. It is clear by these exchanges that the parties intended to enter into an agreement and mutual assent occurred. Plaintiff and Class Members would not have disclosed their Personal Health Information to Defendant but for the prospect of Defendant's promise of medical treatment and other benefits. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' Personal Health Information if it did not intend to provide them with medical treatment and other benefits.

226. Defendant was therefore required to reasonably safeguard and protect the Personal Health Information of Plaintiff and Class Members from unauthorized disclosure and/or use by third parties.

227. Plaintiff and Class Members accepted Defendant's medical services offer and fully performed their obligations under the implied contract with Defendant by providing their Personal Health Information to Defendant among other obligations. Plaintiff and Class Members would not have provided and entrusted their Personal Health Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the

opportunity to control their Personal Health Information for uses other than the benefits offered by Defendant.

228. Plaintiff and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to operate its websites free of surreptitious collection and exploitation of communications between the parties. Defendant failed to do so. Plaintiff and Class Members would not have purchased medical services from Defendant if they knew that Defendant would share their Personal Health Information with Facebook without their knowledge or written consent.

229. Plaintiff and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to operate its websites free of surreptitious collection and exploitation of communications between the parties. Defendant failed to do so.

230. Under the implied contracts, Defendant and/or its affiliated healthcare providers promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' Personal Health Information provided to obtain such healthcare. In exchange, Plaintiff and Class Members agreed to pay money for these services, and to turn over their Personal Health Information through the use of Defendant's websites.

231. Both the provision of medical services healthcare and the protection of Plaintiff and Class Members' Private Health Information were material aspects of these implied contracts.

232. The implied contracts for the provision of medical services—contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Health Information unless they consent—are also acknowledged, memorialized, and

embodied in multiple documents, including (among other documents) Defendant's published Notice of Privacy Practices.

233. Defendant's express representations, including, but not limited to the express representations found in its Notice of Privacy Practices, memorialize and embody an implied contractual obligation requiring Defendant refrain from aiding or allowing third parties to collect or Plaintiff and Class Members' Private Health Information without consent. By soliciting and acquiring Plaintiff's and Class Members' Personal Health Information, Defendant assumed an independent duty to handle Plaintiff's and Class Members' Personal Health Information with due care and consistent with industry standards to prevent the foreseeable harm that arises from a breach of that duty.

234. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Health Information associated with obtaining healthcare private. To customers such as Plaintiff and the Class Members, healthcare that allows third parties to secretly collect their Private Health Information without consent is fundamentally less useful and less valuable than healthcare that refrains from such practices. Plaintiff and Class Members would not have entrusted their Private Health Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Health Information would be safeguarded and protected or entrusted their Private Health Information to Defendant in the absence of its implied promise to do so.

235. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their Private Health Information to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, (a) the

provision of healthcare and medical services and (b) the protection of their Private Health Information.

236. Plaintiff and the Class Members performed their obligations under the contract when they paid for their healthcare services and provided their Private Health Information.

237. Defendant materially breached its contractual obligation to protect the nonpublic Private Health Information Defendant gathered when it allowed third parties to collect and exploit that information without Plaintiff and Class Members' consent.

238. Defendant also materially breached its contractual obligation to protect Plaintiff's and Class Members' non-public Personal Health Information when it failed to implement adequate security measures and policies to protect the confidentiality of that information. For example, on information and belief, Defendant (1) failed to implement internal policies and procedures prohibiting the disclosure of patients' Personal Health Information without consent to third-party advertising companies like Facebook, (2) failed to implement adequate reviews of the software code and java script installed on its websites to ensure that patients' Personal Health Information was not being automatically routed without consent to third party advertising companies like Facebook, (3) failed to provide adequate notice to the public that visitors to its websites risked having their Personal Health Information shared with third party advertising companies like Facebook, (4) failed to take other industry standard privacy protection measures such as providing a "cookie" acceptance button on its website homepages, (5) failed to provide visitors to its websites with a means to opt out of the automatic transfer of data regarding their website interactions to third party advertising companies like Facebook, (6) failed to implement internal policies and educational programs to ensure that Defendants' website managers and coders were familiar with the legal regulations governing the disclosure patient Personal Health

Information to third parties, and (7) failed to install adequate firewalls or take similar measures to prevent the automatic routing of patients' Personal Health Information to third party advertising companies like Facebook.

239. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains, and instead received healthcare and other services that were of a diminished value compared to those described in the contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the healthcare services with data privacy they paid for and the healthcare services they received.

240. As a result of Defendant's material breaches, Plaintiff and Class Members were deprived of the benefit of their bargain with Defendant because they spent more on medical services with Defendant than they would have if they had known that Defendant was not providing the reasonable data security and confidentiality of patient communications that Defendant represented that it was providing in its privacy policies. Defendant's failure to honor its promises that it would protect the confidentiality of patient communications thus resulted in Plaintiff and Class Members overpaying Defendant for the services they received.

241. The services that Plaintiff and Class Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide, which included Defendant's promise that any patient communications with Defendant would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

242. The medical services that Defendant offers are available from many other health care systems who do protect the confidentiality of patient communications. Had Defendant

disclosed that it would allow third parties to secretly collect Plaintiff and Class Members' Private Health Information without consent, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

243. Defendant's conduct in sharing Plaintiff's and Class Members' Personal Health Information with Facebook also diminished the sales value of that information. There is a robust market for the type of information that Plaintiff and Class Members shared with Defendant (which Defendant then shared with Facebook). Indeed, Facebook itself has offered to pay the public to acquire similar information in the past so that Facebook could use such information for marketing purposes. Plaintiff and Class Members were harmed both by the dissemination of their Personal Health Information and by losing the sales value of that information

244. As a direct and proximate result of these failures, Plaintiff and the Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including, without limitation, the release and disclosure of their Private Health Information, the loss of control of their Private Health Information, and the loss of the benefit of the bargain they had struck with Defendant.

245. Plaintiff and the Class Members are entitled to compensatory and consequential damages suffered as a result.

246. Plaintiff and Class Members also face a real and immediate threat of future injury to the confidentiality of their Personal Health information both because such information remains within Defendant's control and because anytime that Plaintiff and/or Class Members interact with Defendant's websites to make appointments, such information about their medical conditions, search for a doctor, or otherwise seek assistance with their medical conditions they

risk further disclosure of their Personal Health Information. Plaintiff and the Class Members are therefore also entitled to injunctive relief requiring Defendant to cease all website operations that allow for the third-party capture of Private Health Information.

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

247. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

248. Plaintiff hereby pleads this Count in the alternative to Counts IV and V.

249. Plaintiff brings this claim on behalf of herself and all members of the Class.

250. Plaintiff and Class Members conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on Defendant in the form of monetary compensation.

251. Plaintiff and the Class Members would not have used the Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to third parties.

252. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

253. The benefits that Defendant derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment

principles for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

254. Defendant should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, ask for judgment in her favor, and that the Court enter an order as follows:

- a. Certifying the Class and appointing Plaintiff as the Class's representatives;
- b. Appoint the law firms of Sweeny Merrigan Law, Keller Postman LLC, and Ahmad, Zavitsanos, & Mensing P.C. as proposed interim class counsel;
- c. Finding that Defendant's conduct as alleged herein was unlawful;
- d. Awarding such injunctive and other equitable relief as the Court deems just and proper, including enjoining Defendant from making any further disclosure of Plaintiff or Class Members' communications to third parties without the Plaintiff or Class Members' express, informed, and written consent;
- e. Awarding statutory damages of \$1,000 per Plaintiff and Class Members pursuant to G.L. c. 272, § 99;
- f. Imposing a constructive trust against Defendant through which Plaintiff and Class Members can be compensated for any unjust enrichment gained by Defendant;
- g. Awarding damages for violations of Plaintiff and Class Members' right to privacy;
- h. Awarding Plaintiff and Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

- i. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law;
- j. Awarding Plaintiff and Class Members reasonable attorney's fees, costs, and expenses;
- k. Awarding costs of suit; and
- l. Such other and further relief to which Plaintiff and Class Members may be entitled.

**RESPECTFULLY SUBMITTED,
COUNSEL FOR PLAINTIFF JANE DOE,
INDIVIDUALLY AND ON BEHALF OF ALL
OTHERS SIMILARLY SITUATED**

/s/ Jonathan T. Merrigan

J. Tucker Merrigan, BBO# 681627
Victoria Santoro Mair, BBO# 679120
Erin E. McHugh, BBO# 703701
Sweeney Merrigan Law
268 Summer St. LL
Boston, MA 02210
Tel: (617) 391-9001
Fax: (617) 357-9001
tucker@sweeneymerrigan.com
victoria@sweeneymerrigan.com
emchugh@sweeneymerrigan.com

Foster C. Johnson (*pro hac vice forthcoming*)
David Warden (*pro hac vice forthcoming*)
Nathan Campbell (*pro hac vice forthcoming*)
AHMAD, ZAVITSANOS, & MENSING, P.C.
1221 McKinney Street, Suite 3460
Houston, Texas 77010
(713) 655-1101
fjohnson@azalaw.com
dwarden@azalaw.com
ncampbell@azalaw.com

Seth Meyer (*pro hac vice forthcoming*)
Alex Dravillas (*pro hac vice forthcoming*)
Keller Postman LLC
150 N. Riverside Plaza
Suite 4100
Chicago, Illinois 60606
(312) 741-5220
sam@kellerpostman.com
adj@kellerpostman.com

Dated: December 8, 2022